Servidores web de altas prestaciones (2016-2017)

Grado en Ingeniería Informática Universidad de Granada

Práctica 4: Asegurar la granja web

Carlos Sánchez Martínez 18 de mayo de 2017

Índice

1.	Instalar un certificado SSL autofirmado para configurar el acceso HTTPS a los servidores.	3
2.	Configurar las reglas del cortafuegos con IPTABLES para asegurar el acceso a los servidores web, permitiendo el acceso por los puertos de HTTP y HTTPS. Esta configuración la vamos a hacer en una de las máquinas servidoras finales (p.ej. en la M1). Se debe poner en un script que se ejecute en el arranque del sistema (poner que se ejecute el script con las reglas del cortafuegos en el archivo /etc/rc.local).	5
ĺn	dice de figuras	
	1.1. acceso Https	4

Índice de tablas

1. Instalar un certificado SSL autofirmado para configurar el acceso HTTPS a los servidores.

Para instalar el certificado SSL se ejecutan las siguientes ordenes en el terminal de un servidor final:

a2enmod ssl

Se reinicia el servidio apache

service apache2 restart

mkdir /etc/apache2/ssl

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Se edita el fichero default-ss y se añaden las lineas: SSLCertificate File /etc/apache2/ssl/apache.crt SSLCertificate Key
File /etc/apache2/ssl/apache.key

Activamos el sitio default-ssl y reiniciamos apache:

a2ensite default-ssl

service apache2 reload

Servidor 1



Apache2 Ubuntu Defa

It works!

This is the default welcome page used to test the correct operation installation on Ubuntu systems. It is based on the equivalent page (Apache packaging is derived. If you can read this page, it means the installed at this site is working properly. You should **replace this fil** /html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this p that the site is currently unavailable due to maintenance. If the prol site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstreinto several files optimized for interaction with Ubuntu tools. The codocumented in /usr/share/doc/apache2/README.Debian.gz. Redocumentation. Documentation for the web server itself can be four apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on l

```
/etc/apache2/
|-- apache2.conf
```

Figura 1.1: acceso Https

2. Configurar las reglas del cortafuegos con IPTABLES para asegurar el acceso a los servidores web, permitiendo el acceso por los puertos de HTTP y HTTPS. Esta configuración la vamos a hacer en una de las máquinas servidoras finales (p.ej. en la M1). Se debe poner en un script que se ejecute en el arranque del sistema (poner que se ejecute el script con las reglas del cortafuegos en el archivo /etc/rc.local).

Priemro habilitamos el puerto para ssh con las ordenes: iptables -A INPUT -p tcp -dport 22 -j ACCEPT iptables -A OUTPUT -p udp -sport 22 -j ACCEPT Habilitamos el protocolo HTTP con la orden: iptables -A INPUT -m state -state NEW -p tcp -dport 80 -j ACCEPT Habilitamos el protocolo HTTPS con la orden: iptables -A INPUT -m state -state NEW -p tcp -dport 443 -j ACCEPT Bloqueamos el tráfico ICMP para evitar ataques ping de la muerte: iptables -A INPUT -p icmp-type echo-request NEW -j DROP Salvamos la configuración de iptables: service iptables save Iniciamos iptables: service iptables start Para ejecutar nuestro script cuando arranque el sistema vamos a modificar el archivo rc.local y añadimos la linea:

sh nombre script

```
Hybin/bash
Imyscript.sh
Habilitamos el puerto para ssh
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p udp --sport 22 -j ACCEPT
iptotocolo HTTP
iptables -A INPUT -m state -state NEW -p tcp --dport 80 -j ACCEPT
improtocolo HTTPS
iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
ibloquear el trafico ICMP para evitar ataques ping de la muerte
iptables -A INPUT -p icmp-type echo-request -j DROP
service iptables save
service iptables start
```

Figura 2.1: Configuración iptables